CITRIX®

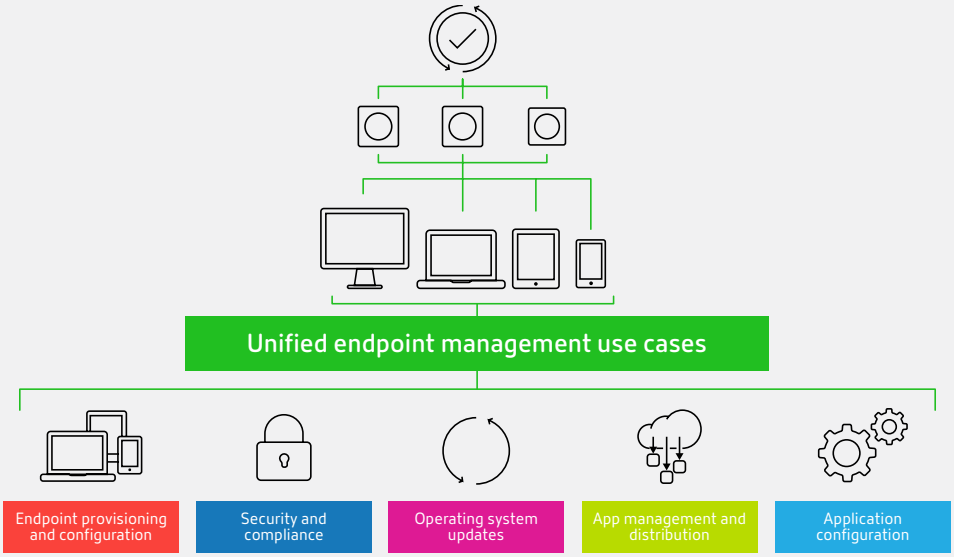
White Paper

Unified endpoint management: The modern way to secure and manage your devices

Table of contents

Today's employees are mobile — and it's forcing the workplace to evolve. As IT shifts from stationary desktops to roaming laptops, tablets, and smartphones, many organizations are finding the tools they once relied on are no longer enough.

Instead of controlling and securing different devices across diverse platforms, there's now a simple way to manage them from a single console. Welcome to the age of unified endpoint management (UEM) — the modern style of management.



Why UEM?

Simplicity

In the past, organizations had to rely on separate client management tools (CMT) and endpoint management (EMM) technology to manage their endpoint infrastructure. Now, unified endpoint management (UEM) brings the capabilities of CMT and EMM together into a single solution, allowing IT to easily secure and manage apps, data, and operating systems across your enterprise.

Because CMT and EMM tools have significantly different ways of working, they typically require a separate set of staff and training for each. Conversely, managing all your devices from a single tool makes better business sense. Not only is it less expensive to invest in one management tool instead of two or three, but it also significantly increases operational savings by reducing the need for staff resources and training. As a result, your existing staff can be leveraged for more strategic purposes.

Consistency

In management, consistency, security, and usability are essential for user productivity and information protection. Even small, unintended differences in security and management policies can leave holes in the infrastructure that allow hackers and malware to penetrate the organization. Having consistent policies makes it easier to identify, correct, and monitor any gaps. Consistency in mobile access to applications and information is also important for user productivity.

A few of the ways UEM delivers consistency:

- Approaches to systems, like troubleshooting and user help desk services become uniform.
- Operating systems, such as Windows 10 or macOS, have more consistent interfaces across different types of devices.
- Customers can easily manage their legacy Windows 32 applications through a UEM solution delivered via a Citrix Workspace — over the entire application lifecycle. (i.e., app deployment, app configuration and uninstall, if needed)
- Reporting is easier and more comprehensive, giving IT deep insights to help improve usability and performance.

Device-friendly management

CMT tools were conceived at a time when desktops, laptops, and devices were stationary, corporately distributed, and mostly connected to the enterprise LAN. Because they had to be joined to an enterprise domain with group policy for initial configuration and subsequent management to take place, a user could not typically connect, configure and upgrade his or her own device. Maintenance was the job of IT, who acted as the ultimate superuser.

Some organizations still use CMT solutions, and it means IT spends a lot of time creating anywhere from one to a few sets of custom system images and pushing them over the LAN to a few, scores, or hundreds of network-connected desktops and laptops. With such a methodology, on-boarding new devices, or replacing a lost or stolen laptop with all the necessary applications is a resource and time-consuming process that hampers user productivity.

Because CMT application packages are customized causing complex distribution packages they require higher level of support. By contrast, UEM APIs and tools were designed to support roaming, wirelessly connected mobile users on their chosen devices. They also mean:

- Users can acquire a device with a vendor-configured operating system. Using an enterprise UEM portal and configuration app, users can register and configure their own devices over wi-fi or a cellular connection — all with little or no help from IT.
- Users can also use a corporate app store portal to download and install IT pre-approved applications.
- When necessary, IT can push out updates to globally roaming devices across cloud, SaaS, and virtual applications.

Security and productivity through containerization

Bring-your-own-device (BYOD) is now a significant trend because it offers a considerable cost savings to organizations. However, mixing data between BYOD and corporate-owned-personally-enabled (COPE) devices puts organizations at risk. Containerization is one of the ways UEM allows BYOD and COPE workstyles. Using application wrapping, encryption and other similar methods, IT can separate corporate and personal apps and data on each device, restricting or disabling interactions between the two based on the security policies set by the enterprise.

Containerization also accomplishes both malware protection and data leakage prevention (DLP). Since enterprise and personal applications and data on the device are walled off from each other, any malware downloaded with personal applications or browsing has no impact on containerized enterprise applications and cannot be transmitted to the enterprise network when the device connects.

Another way containerization protects against data leakage is through the configuration and enforcement of policies that regulate users' ability to cut and paste data from enterprise to personal applications, paste or attach enterprise data or files to personal email messages, and print files containing sensitive data.

How Windows 10 is different

With Windows 10, containerization can be accomplished via digital rights management through the enforcement of Windows Information Protection (WIP) encryption of all enterprise applications and data. IT can then leverage policies that prevent users from cutting and pasting encrypted content into unmanaged applications not using WIP encryption, including personal email client software.

A UEM designed to work with Windows 10 helps drive other critical management features, and can:

- Push down and enforce a raft of policies and settings
- Enforce password and encryption on any data downloaded from services, such as SharePoint or a shared network
- Enable self-enrollment of new devices through Azure Active Directory
- Manage corporate provisioned apps separately from user installed apps, distribute Windows 32 apps via .msi packages
- Enforce and deploy updates
- Prevent access to dangerous websites

All of this is done without having to touch the device connecting it to the enterprise LAN. And, any 32-bit Windows application that can't be leveraged this way can be deployed to mobile devices via desktop virtualization solutions.

How Apple macOS is different

With OS High Sierra, Apple also started giving the desktop operating system most of the same policy-based, self-enrollment management APIs as iOS — and more will come with macOS.

Citrix Workspace—a UEM solution for all needs

Citrix provides a comprehensive, integrated UEM solution to manage multiple platforms including iOS, Android, Windows 10, and macOS devices, including desktops, notebooks, and Chromebooks, and support for IoT tools and devices, such as Citrix Workspace Hub and Alexa for Business. As a part of the Citrix Workspace, Citrix Endpoint Management combines UEM with apps and desktop virtualization, file sync and share, secure network gateway services, plus security and productivity enhancements to Office 365.

A mobile VPN helps prevent malware-infected apps from accessing resources behind the firewall. It also provides unique Mobile Device Identifiers assigned at the app level — not just the device level — to monitor, filter, and block individual connections or devices. This integration provides access to Office productivity apps along with all other apps users need — including legacy Windows apps, SaaS, web and mobile apps — and all are available to users from a unified app store.

Support and security

Citrix Endpoint Management delivered via Citrix Workspace provides increasing support for all operating system enterprise management APIs as they are introduced. It also adds its own unique capabilities that give management consistency across device operating systems. These include encryption and containerization features on top of those offered by operating system APIs and its own toolkit and SDK for wrapping individual applications to protect their associated sensitive information. This ensures a seamless, productive experience for the user plus consistent, necessary protections for the enterprise.

Citrix Secure Mail

An enterprise email client and personal information manager with a user-friendly interface, Citrix Secure Mail is much like those of device-native email client solutions — with scores of additional features that enhance security and usability in an enterprise setting. With Citrix Secure Mail, all corporate email, contacts, and calendar items are stored separately from the personal applications on the device. Futhermore, Secure Mail:

- Can be accessed via single sign-on after the user logs into Secure Hub
- Offers multifactor authentication, remote wipe, and encryption in transit and at rest
- Has enforcement restrictions on email attachments, and printing and cutting and pasting of information from other applications into emails
- Integrates with organizations' existing data leakage prevention (DLP) tools, which monitor and restrict content sent out in enterprise emails

What's more, Citrix Secure Mail tightly integrates with the Citrix Secure Web mobile app so that email web links are opened in a secure, sandboxed, environment to minimize threats. And it also integrates with our content collaboration service, making it easy to embed links in email rather than attaching files, for tighter control over content sharing.

Citrix Secure Mail also offers outstanding convenience features that enhance your users' experience, such as viewing the availability of meeting invitees, and a simple, single touch to join online meetings.

Citrix Secure Web

A secure browser that IT can use to place policies and restrictions on web browsing, Citrix Secure Web is particularly beneficial when connecting to the corporate network and intranet. Organizations can apply policies that govern which websites users can and cannot access, what enterprise firewall proxies are used to access them, and can analyze and filter URLs to ensure they're safe. This helps protect organizations from web-based threats, especially when users are on public Wi-Fi.

Citrix Content Collaboration

Citrix Content Collaboration is an enterprise-class secure mobile file sync and share application, that provides enterprise-grade features, security, and management — and is more convenient than consumer-friendly Box and DropBox. Rather than forcing users to store all information in the cloud, organizations can leverage storage zones to store shared files either on-premises behind the firewall, in the Citrix Content Collaboration cloud service, or in another public cloud storage service of their choice. Citrix Content Collaboration also:

- Provides connectors for Windows network shares and Microsoft SharePoint, so files don't have to be migrated to another service to be shared
- Offers an easy-to-use solution that novices can use to create, populate and store mobile forms-based applications running on a variety of devices
- Helps organizations digitize and automate manual workflows and processes rapidly, improving productivity and eliminating double data entry and paperwork in the field
- Integrates seamlessly with other Citrix and non-Citrix productivity applications
- Leverages all the robust security and management features of Citrix Endpoint Management to protect and secure enterprise data

Citrix Workspace app

This universal app gives your teams centralized access access to all their web, mobile, SaaS, Windows and Linux apps, desktops and files — all with an easy-to-use, all-in-one interface.

Embracing IoT with Citrix Workspace

Citrix Workspace also extends mobility management into evolving technology. IoT-enabled workplaces can synthesize data from different sources to respond to user needs — increasing workplace efficiency and productivity as a result. For example, proprietary Citrix software can automate workspace functions, like launching a personalized desktop when a user approaches a workstation; adjusting room temperature and lighting, starting a virtual meeting when staff enters a conference room, or using beacons to connect users automatically to nearby printers. This emerging technology ensures your organization will be ready to adapt to the future of work quickly.

Moving your business forward with Citrix Workspace

Citrix Workspace makes it possible to simplify, secure, manage, and monitor all types of endpoints, applications, and software from a single pane of glass. Unique to Citrix, the entire workspace has contextual security with end-to-end analytics

across infrastructure, apps, networks, and devices for unparalleled monitoring. For your end-users, Citrix Workspace provides a single point of entry to the apps and data they need to be productive and collaborate on any endpoint.

Our complete UEM solution not only integrates management, security, application and desktop virtualization, and mobility into a centralized infrastructure, but it also provides a framework and enterprise-grade IoT enablement — so your company is ready for the technology ahead. What's more, our cloud technologies allow you the flexibility to increase or decrease infrastructure with your changing business needs. Delivering UEM via Citrix Workspace as a service is the fastest, simplest and most flexible way to securely bring digital workspace technologies to your organization.

Find out how we can help simplify administration of your workspace at Citrix.com/UEM

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States